

Abort, Retry, Ignore...



May 2005

Suggested Retail Price \$1.95 Volume XXI

Issue 05

Calendar
of
Events

!!! IMPORTANT !!!

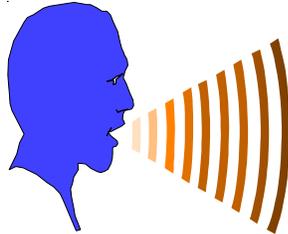
Meeting date
Saturday
May 28
Time 9:45 - noon

MEETING PLACE
will be the
Glenside Public
Library

SEE YOU
THERE!!

COD
Computer
Show Dates

2005
May 22
June 26
July 31



CAEUG website has a new home.

Remember to change your bookmark to the new address.

<http://www.caeug.net>

TABLE OF CONTENTS

CAEUG NEW WEBSITE ADDRESS1
HELPLINE.2
DOUBLE THREAT ON LINE TRAVEL SCAM BY IRA WILSKER3
CURRENT HOAXES AND URBAN LEGENDS BY IRA WILSKER5
THE LAMP POST - NUMBER 62 BY JOHN SPIZZIRRI6
WHY THE CHANGE BY JOHN SPIZZIRRI9

CAEUG OFFICERS & CHAIRPERSONS



President	Mike Goldberg
V.P. (Programs)	Frank Braman
Secretary (& donuts)	Dean Holste
Treasurer	L. Johnson
Newsletter Editor	Kathy Groce
Membership Chairperson & Circulation Manager	Pete Nicchia
CAEUG COD Coordinator & Publicity	Terry Moye
Software Reviewer	Brian Noon
Webmaster	
& Technical Consultant	John St. Clair
Coffee Service	Joan Thompson
Picnic Chairpersons	Mike Goldberg Roger Kinzie

Reminder: You'll get better, faster service if you use CAEUG in the subject of your e-mail.

ABOUT THE NEWSLETTER:

This printed version of our newsletter was laid out using **Adobe's Pagemaker Version 7.0** for Windows and was printed on a **HP Laserjet III**. Our group's membership database is maintained using **MS Access** and address labels are printed using **MS Access** software. Our checking account records are kept in **Quicken** software.

The opinions expressed in this newsletter are not necessarily those of the CAEUG Officers, members or other contributors. CAEUG, its officers, newsletter editor, authors or contributors are not liable in any way for any damages, lost profits, lost savings, or other incidental or consequential damage arising from the use of the information provided herein. Every reasonable effort has been made to confirm the accuracy of the contents of this newsletter, but that accuracy is not guaranteed.

Permission is granted to reproduce any or all parts of this newsletter for personal use. Also granted is permission to reproduce for publication any part of this newsletter provided that a copy of the publication is mailed to CAEUG, immediately following publication and CAEUG is given credit.

The CAEUG newsletter is published eleven times annually. Contributions by members are encouraged and will be gratefully acknowledged in the newsletter. We have a policy of exchanging newsletters with other users groups across the nation. Several CAEUG member articles have already been picked up and reprinted.

Membership Costs.....

	First Yr.	Renewal
Individual	\$25.00	\$20.00
Family	\$30.00	\$25.00
Corporate	\$30.00	\$25.00
Associate	\$20.00	\$15.00

Beginner's SIG

Ask questions and discuss computer experiences with this group.

Such as:

1. New to Computers? (basic topics)
2. How to use the Web or download information
3. How to install hardware/software
4. Discuss how to troubleshoot hardware conflicts, learn boot up emergency tricks
5. What do you want to know??

SIG meets before regular meeting from 9:05 to 9:45

MEMBERS HELPLINE

Any member with a specific expertise can volunteer to be on the Members Helpline.

Beginner Helpline Billy Douglas

Beginner hardware problems . Dick Fergus

QuickBooks, Turbo Tax, IBM Lotus, MS Excel, Corel's Quattro Pro . . . Terry Moye

Hardware problems, Win 9x, 2K, XP & Linux John Spizzirri

**Great Midwest
Computer Show**

**Next show date
SUNDAY May 22
College of Dupage
9:30 A.M. to 3:00 P.M.**
*The Midwest's oldest and largest
Multi Vendor PC show and sale for
Home & Business*

COLLEGE OF DUPAGE
Main Arena of Physical Education Building
Corner of Park Blvd & College Road
Glen Ellyn, IL

**FREE PARKING
Admission - \$7.00
Kids 12 and under FREE**
<http://www.greatmidwestcomputershow.com>
**E-mail address:
info@greatmidwestcomputershow.com**

**Great Midwest Computer Show ©
2005 dates**

May 22, 2005 at COD
June 26, 2005 at COD
July 31, 2005 at COD
August 28, 2005 at COD
September 25, 2005 at COD
October 30, 2005 at COD
November 20, 2005 at COD
December 18, 2005 at COD

**NEW Money Saving Offer for CD of the Month
Pre Order + Prepay = SAVE \$\$**

The club will offer the CD of the Month on a pre order, prepaid basis. The charge will be \$50.00 a year for 10 months. This is \$20 annual savings over buying them for \$7 each month. Lynn Johnson, the treasurer, will keep track of anyone placing a 10-month order. Anyone wishing to place a prepaid order should contact:
Lynn

Double Threat Online Travel Scam

By Ira Wilsker

**APCUG Director and Columnist, The Examiner, Beaumont TX
iwilsker@apcug.net**

Most of us like to travel, and would especially enjoy a travel bargain. We may have checked with reliable travel resources such as our local travel agents, airlines, cruise lines and hotels but were unable to find the deal that we wanted. We check the major travel sites such as Expedia, Orbitz and Travelocity, but still can not find a deal that makes us happy. Since we are experienced Internet users, we go to the major search engines such as Yahoo, Google or Alltheweb, and search for bargain travel sites. We notice some websites that appear at the top of the listings, sometimes in the premium paid listings on the search engines, that allege airline tickets, hotel rooms, and cruises at far below the prices charged by the reputable sources that we are familiar with, so we click on the links. One link may be for CheapClouds.com, claiming deep discounts off published fares; another link may be for Busysky.net that offers comprehensive travel services with fares far below those offered by travel agents or other online travel websites. Two other websites offering unbelievable travel bargains that appear in the paid or premium listings on the search engines are Crazytickets.net and Submitprice.net.

Tasting a good deal, we click on one of these sites and see a travel site similar to the better-known and reputable sites with which we are already familiar.

We search for fares and find tickets for about half of what we would pay elsewhere; we find hotels and cruises similarly priced. Unable to resist such bargains, we select our trips and we are asked to enter our credit card information. A familiar window appears that asks us for our credit card number, security code (the three or four digit code on the credit card), expiration date, and name on the card. With a sense of excitement, we eagerly await the confirmation, which we are told may take a few minutes, but are instead presented with an official looking window that says that our credit card information could not be processed. We are then presented with an option to pay with another credit card, or pay by an alternative means. Thinking that it is just a simple glitch, and not wanting to lose the

(con't on page 4)

opportunity for a glorious vacation at a bargain price, we enter the required information for another credit card. We are again greeted with the same screen that it could not be processed, and are then told to contact customer service by email, utilizing the link and transaction number provided on the screen.

A short time later, we will receive an email from the travel company apologizing for the inconvenience, and claiming that their bank is having trouble processing credit cards. Since the price quoted is only valid for a very short time, the traveler is asked to use alternative methods of payment - wire the proceeds via Western Union. Readers of this column may feel a hint of skepticism at this point, remembering that sometime ago I wrote that while a legitimate method of sending money, wiring money via Western Union to pay for Internet purchases should raise a red flag of suspicion. Still, eager not to let the bargain of a lifetime get away; we follow the instructions on the email from customer service. The address to wire the money to may raise more suspicions, as the destination is not in the United States, but instead in Bulgaria, Romania or Thailand. An inquiry email back to customer service may bring a prompt canned reply that the reason why the deal is so good is that these prices are only available for tickets purchased outside of the U.S., along with an assurance that they will be honored by the airlines, cruise lines, and the hotels. Still not wanting to lose out on this dream vacation, we send the money via Western Union, exactly as requested. We will then receive an email stating that it will take several days to receive our tickets, and are provided with a web link and tracking number to show our tickets are on the way.

After not receiving the tickets in the time specified we click on the tracking number, and are given another canned response that they are being processed, and should be delivered in the next few days; following up clicks several days later display the identical statement. An email reply from customer service reiterates the message. By the date of the dream vacation, no tickets have arrived, dashing any dreams of a good time.

We have become the victims of another very nasty scam circulating on the Internet. What is

especially insidious about this scam is that it is a "double whammy," in that we are not only out of the money for the trip, since the money sent via Western Union is virtually unrecoverable, but we have also given unscrupulous unknown parties our credit card information!

This is not some fictitious scenario by a mystery writer but a documented scam. The scam has become so pervasive that even some of the antivirus companies have posted warnings about it on their websites. There is anecdotal evidence that, in several of the cases, the victims' credit cards had been illicitly charged for a variety of goods and services in the days immediately following the fraudulent transaction, possibly committed by the same travel thieves.

The websites mentioned above were real, and are well documented, but are currently offline (as I type this). Based on their success at defrauding countless victims, it is likely that they will reappear under different names.

In order to be safe when shopping for travel bargains, be sure to use a reputable resource, such as a local travel agent, airline or hotel website, or trusted third party website. If you pay with a credit card, there is some degree of protection from fraud from the credit card company. Never wire money, especially overseas, to pay for a travel bargain. We work too hard for our money to have miscreants steal it from us under the false pretenses of a travel bargain.

The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.

Several articles in this newsletter have been provided by The Editorial Committee of APCUG.

Special thanks for their contribution to computer club newsletters.



**Current Hoaxes and
Urban Legends**
By Ira Wilsker
APCUG Director and Columnist
The Examiner, Beaumont TX
iwilsker@apcug.net

WEBSITES:

<http://www.snopes.com>

<http://urbanlegends.about.com>

Some of us find them cute, entertaining, exciting, and fun, while others of us find them embarrassing, irritating, and a waste of time. Many forward them believing that they are doing good, or warning of harm, or forward them because they came from an allegedly reliable source. A few are so convinced of their truth that I am explicitly requested to put them in this column, or announce them on my radio and TV show. What I am referring to are the hoaxes and urban legends currently circulating on the internet that many of us seem to love to forward to everyone in our email address books. Many of these hoaxes and urban legends have a grain of truth or logic in them, while many others are totally lacking any basis in fact, yet many of us still enjoy forwarding them without a second thought.

In order to avoid embarrassment I strongly recommend that everyone tempted to forward such emails should check out their validity prior to another mass send to all we know. There are several excellent websites that compile information on these emails, and a quick check can save us from the embarrassment of sending out a hoax, and preserve our personal credibility. If we find that the interesting email is indeed true, we should still consider not forwarding them to everyone, as many of our intended recipients may not find our interests to their likings, and may even be offended that we consumed their valuable bandwidth and time. Typically, when I receive one of these from an acquaintance, if I am not already familiar with it, I check it out; if it is true (a minority of the time), I may choose to selectively forward it only to those that I think may be interested in the topic, but I never send it to everyone in my address book. If it is false, I usually reply back to the sender that it is indeed false, and include a link

documenting the falsehood. Some emailers are so humiliated that I caught them in an inaccuracy that they reply in anger back to me, despite the incontrovertible fact that it was they who had sent the bogus email.

To verify the authenticity or falsehoods of these oft forwarded emails, I use two primary, and several secondary resources. Primarily I use the excellent and comprehensive urban legends resource of Snopes, at www.snopes.com. Well organized in an easy to navigate menu format, along with a competent search engine makes Snopes an excellent choice to check out the validity of questionable emails.

My other primary resource for checking the legitimacy of potential hoax emails is urbanlegends.about.com. This site is frequently updated with the latest hoaxes in circulation, and can reliably document their validity.

A common topic of these questionable emails is virus warnings. For this reason, most of the major antivirus software publishers also compile lists of hoaxes, mostly virus related, on their websites. I utilize these sites as secondary resources. It is also notable that old hoaxes and virus warnings never seem to die out, and periodically reappear. One that has been documented to be in circulation for over six years, but is again currently making the rounds in mass emailings is the "It takes guts to say Jesus" virus hoax. This email, in several iterations, warns that according to CNN, AOL, McAfee, and other reputable resources, that there is an email circulating with a virus that can not be detected by contemporary antivirus software and that if you open the email, your computer will be effectively destroyed. Every one of the hoax and antivirus websites list this as a hoax, yet countless copies are being forwarded by well intentioned people trying to warn their acquaintances. Some of the variations even go on to state that while it may be false, it is so important that it is being forwarded anyway. Another similar email warning that does have some validity is the one that says "I've Got Your E-mail on My Account". It goes on to warn that someone is using "your" email account to spread a virus, and I have received 10 copies of it, all with your email address and ISP in the header. The email then says, "I have copied all the

(cont'n on page 6)

mail text in the windows text-editor for you & zipped then. Make sure, that this mails (sic) don't come in my mail-box again." Attached to this dire warning is a file, commonly named "your_text.zip". If opened, the file will infest your computer with the Sober.N worm. If it infects your computer, Sober.N will terminate the antivirus and firewall software on your computer, rendering it vulnerable to further attack, and then forwarding itself to everyone in your address book! This Sober.N warning is the exception to the rule that most warnings of this type are bogus.

Another dire warning, which I am receiving multiple copies of, is the warning that a directory of cell phone numbers is being compiled to enable telemarketers to call us on our cell phones, consuming our valuable supply of limited minutes. This hoax, which is now circulating for the second time, is listed by several sites as one of the top hoaxes in circulation. The grain of truth in this is that most cell phone carriers are instituting a "411" directory service of cell phone numbers, this list will emphatically not be for sale to telemarketers.

To see the latest hoaxes in circulation, as well as the ones in widest distribution, check out the hoax and urban legend websites, or the website of your favorite antivirus software. You may find some of the hoaxes actually quite entertaining, and wonder how intelligent people could fall for such silly emails.

The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.

The Lamp Post
Number 62 by John Spizzirri
May 22, 2005



There is a ray of sunshine in the Choicepoint affair. You will recall from previous columns that Choicepoint sold the personal information of about 300,000 people to criminals. PrivacyActivism, an organization in San Francisco, reported that in a VERY small sample of dossiers, the data was largely incorrect. The story is at <http://www.privacyactivism.org/Item/222> .

The price of popularity is cracker attacks. Firefox, the Mozilla browser (<http://www.mozilla.org>), is enjoying its 50 millionth download. Its popularity has also engendered a number of attacks. Mozilla has been alerted to 4 serious security flaws in the last 5 months. In each case the flaw was fixed within two to three weeks. Compared with Microsoft (MS <http://www.microsoft.com>), Mozilla acts to correct problems at light speed. Mozilla does not conceal problems, either. MS defenders are now saying "We told you so" about Open Source Software (OSS) stability and safety. I think the Mozilla track record is excellent. When they are notified of a bug, they take ownership of the problem and fix it as fast as possible. MS, on the other hand, attacks the people who notified them of the bug (Eeye, for example). MS takes months to fix the problems in Windows and Internet Explorer (IE). I hereby reply to the MS defenders. I told you so, OSS is better than proprietary MS products.

MS does not like Linux. It uses its investment in Santa Cruz Operation (SCO <http://www.sco.com>) to sue the proponents of Linux (IBM <http://www.ibm.com> and Novell <http://www.novell.com>). Now it is going after consumers. The company has come up with the "Windows Validation Tool" which detects the use of Wine. Wine is a program that runs on Linux that allows users to operate Windows programs on the Linux system. If the tool fines Wine, it

generates an error. Its funny that MS purchased a product that is similar to Wine and VMWare, but does not promote it. VMWare is a product which is unaffected by the validation tool. VMWare was just purchased for 600+ million dollars. The reports of this purchase, that I have heard say, it was a steal. The previous owners of VMWare still run the company. Maybe MS is just against non-profit organizations. The story is at

<http://ct.eletters.whatsnewnow.com/rd/cts?d=181-411-1-278-33238-18555-0-0-0-1>

Computer Business Review Online reports that Cuba is converting government offices to Linux. The story at

http://www.cbronline.com/article_news.asp?guid=9B077C17-C2F9-4472-8B28-25F0B19E2F8A does not explain how MS can sell any of its products to a country the US does not recognize as a country.

If Windows XP crashes, you get a message stating that the error was detected and asking if you want to send information about the crash to MS. Unless you are plagued by crash after crash, I would advise NOT sending data about the crash to MS. The data that will be sent to MS may include personal information that you have on your machine. The question that came to my mind is, "Who will see this data?" I checked the Microsoft online crash analysis page at

<http://oca.microsoft.com/en/dcp20.asp> . On that page MS indicates the people that may see your personal information may include, "Microsoft employees, contractors and vendors who have a business need to use the error report data are provided access. If the error report indicates that a third-party product is involved, Microsoft may send the data to the vendor of that product, who may in turn send the data to sub-vendors and partners." That statement gives MS carte blanche to give your information to just about anyone they choose. I may be paranoid, but I do not trust various "contractors", "vendors", "sub-vendors and partners" who's names I will never know.

The amount of child seduction on the Internet is not proportional to the headline cases we see in the press. It is much greater. To see a fraction of the vast quantity that is happening every day look at **<http://www.perverted-justice.com/>** . This site was featured on Kim Komando's radio show (**<http://www.komando.com/>**). It has the nick name PeeJ. It has actual chat room conversations between unprosecuted pedofiles and people passing themselves off as children to assist law enforcement and post conversation texts of these perverts. It has pictures of busted pedofiles associated with these conversations. WARNING: This site has the exact language used in these IM (Instant Messaging) conversations which includes unthinkable situations and dirty words. Don't view this site unless you are prepared for what you might see. This site is definitely NOT for children. It is very unsettling.

Kim Komando also had a tip of the day about the hosts file,

http://komando.com/tips_show.asp?showID=8826 . The hosts file is a file that Windows uses to speed delivery of Internet content. It can be changed to prevent going to sites that have bad content or spyware. She recommends the use of a custom host file located at

<http://www.mvps.org/winhelp2002/hosts.htm> that blocks the bad sites for you i.e., saves you the work of doing it yourself. Instructions include where to place the file. That custom file will be on the CD of the Month with the instructions.

The Avon and Somerset Constabulary (A&SC) in England has its own Web site. In England the emergency phone number is 999. It is equivalent to 911 in the United States. On the A&SC Web site there are audio and transcripts of calls to 999 that should not have happened. They post these on the site as an example of what calls should not be made to 999. Some of these calls are very funny. Check them at

http://www.avonandsomerset.police.uk/communications/examples_of_999_calls.asp .

(con't on page 8)

Smoke and mirrors, dog and pony show, and slight of hand all refer to magic shows and politics. The debate over John R. Bolton's appointment to the United Nations, the fight over the President's federal judicial appointments, and trips to Iraq by Laura Bush and others take our attention away from issues that will affect our daily life. The Real ID bill was brought up last year and soundly defeated. It was brought up again this year and soundly defeated. It was then attached to the "Iraq Supplemental Spending Bill" and was passed with almost no opposition. Senator Durbin made speeches against the Real ID for reasons related to immigration, see

<http://www.aila.org/contentViewer.aspx?bc=9%2C594%2C8140%2C9251> . The full text of the bill is at <http://thomas.loc.gov/> by searching **HR1268** . The President signed the bill under the name "Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005" the day after it was passed, see

<http://www.whitehouse.gov/news/releases/2005/05/20050511-5.html> . In section 202 of the law, the Secretary of Homeland Security has the authority to require minimum standards of state issued ID cards and drivers licenses including "common machine-readable technology, with defined minimum data elements". It looks like we will have RFID whether we like it or not. Another requirement is "Proof of the person's social security account number or verification that the person is not eligible for a social security account number". If you have ever read your Social Security card, it plainly states "not for identification". The states will be able to get "grants" to offset the costs of becoming compliant. If a state chooses not to be compliant, state issued ID cards will not be acceptable for any federal transaction like getting on an airliner. Other sites that have information about this issue are <http://www.unRealID.com/> and <http://www.strike-the-root.com/51/morris/morris5.html> .

Can you identify a serial killer? I found an amusing online quiz that shows pictures of programming language inventors and serial killers and asks you if you can identify which is which. Find the quiz at <http://www.malevole.com/mv/misc/killerquiz/> .

The latest issue of 2600 Magazine (<http://www.2600.com/>), volume 22 number 1, has a excellent article about "scumware". The writer, "LoungeTab", has one term for adware, spyware, and sneakware. (I will refer to LoungeTab as he for simplicity.) He calls it scumware. He describes the removal tools and how to use them. All the tools he describes are on or have been on the CD of the month with the exception of KazaaBegone and IEeradicator. He notes that MSCONFIG is very useful in getting rid of scumware but is not standard in Windows 2K. He states that any version of it works in Windows 2K. The WinXP version, which he recommends, is available at <http://downloads.thetechguide.com/msconfig.zip> . There is quite a bit of useful information at The Tech Guide site - <http://www.thetechguide.com/> . There are many how-to's, tweaks, and downloads (primarily Linux iso's).

I, occasionally, get an e-mail from someone I know that has been forwarded at least once. Some of these e-mails have extraordinary stories. If I have not seen the story before and want to check if it is true, I go to <http://www.snopes.com> . Snopes and other Web site keep track of these type of stories and check the facts. Their Web site is an authority on urban legends and scams. For instance, <http://www.snopes.com/crime/dumdum/gunshop.asp> is the story about a stupid criminal that committed an armed robbery of an open gun shop. The facts in the case sound preposterous. The criminal was killed at the scene by the clerk and six other armed customers in a hail of gunfire (23 wounds). Snopes checked the facts and found that the criminal was, indeed, stupid and dead. He robbed a gun store near Seattle, WA. The robber was killed by the clerk and a uniformed police officer customer with four shots. The e-mail had exaggerated the story. In another instance, an e-mail story claims that there is a bathroom with a floor mural of a view from an aircraft giving the illusion of falling from a great height (<http://www.snopes.com/photos/arts/bathroom.asp>). Snopes checked the facts finding this false.

The bathroom picture is actually an altered photograph from a contest by <http://www.worth1000.com> . Another e-mail details a site that may be used to snoop on you <http://www.snopes.com/computer/internet/zabasearch.asp> . The explanation says the e-mail is essentially true but may be a marketing gimmick for <http://www.zabasearch.com/> . If you receive an e-mail with an interesting story and want to check its validity, go to Snopes.com and search for the unique aspects of that e-mail. By the way, you can check what new e-mails are making the rounds by going to Snopes.com and clicking the "What's New" button.

For the last two years since Bill Gates declared that security would be MS's main goal, MS has fumbled around trying to tighten the security holes in Windows, Internet Explorer, Office, and Windows Media Player with little success. In this ZDNet article, http://news.zdnet.com/2100-1009_22-5705430.html?tag=nl.e589 , is a revealing sentence that may explain their ineptitude. The article introduces another new product that will take care of security automatically called "Windows OneCare". In the fifth paragraph it says matter of factly "the company is seeking to establish an ongoing billing relationship with customers". There you have it. Pay more money so their products will work safely and correctly. I guess its like buying an extended warrenty on a car or paying protection money to the mafia.

Businesses are under attack on their use of e-mail. E-mail policies and the e-mail itself are being used for evidence in criminal and civil litigation against businesses. This article, <http://www.it-director.com/article.php?id=12710> , details what is being done and what needs to be done. If you use e-mail at work or are responsible for e-mail policy, this article is worth reading.

MS Office 12 will be released in mid summer next year as reported by The Register, http://www.theregister.co.uk/2005/05/12/_office_2006/ . The new version will have many new features that virtually no one will use. According to the article, 30% of MS Office users are using version 97. Sun Microsystems, <http://www.sun.com/> , will release version 8 of Sun Office this summer that promises to work better with MS Office files. Open Office, <http://www.openoffice.org/> , have introduced a beta version (2) of Open Office.

I found this one on the Orange County IBM PC Users Group (<http://www.orcopug.org>), "If you play a Microsoft CD backwards it plays satanic messages. Worse yet, if you play it forwards it installs Windows."

Between you, me and The Lamp Post that's all for this month.

Why the Change??

by John Spizzirri

We have changed the name of our Web site from CAEUG.ORG to CAEUG.NET. Due to a miscommunication and a time delay in getting information to the registrar, our registration of the caeug.org name was cancelled. A Miami company that buys expired registrations in anticipation of selling them back to their original owners bought caeug.org. I contacted them via e-mail asking what price they wanted for our name. They responded with a price of \$2900.00. I did not respond to their e-mail because of the ridiculous price. What I did instead was purchase the name caeug.net for ten years. Ten years will allow us to have an established Web presence. I will set up annual procedures that will prevent a situation like this from happening again. I regret this change, but I think it was necessary under the circumstances. Be sure to check out the site at <http://www.caeug.net> .

CAEUG
P. O. Box 2727
Glen Ellyn, IL 60138

FIRST CLASS MAIL

Meeting place and date information:

The next REGULAR meeting will be held at the
Glenside Public Library in Glendale Heights
starting 9:45am on
Saturday May 28

The library is located. Please park at the West side of the lot, away from the building. Thank you. The meeting(s) are not library sponsored and all inquiries should be directed to Mike Goldberg. Individuals with disabilities who plan to attend this program and who require certain accommodations in order to observe and/or participate in the program are requested to contact CAEUG president, Mike Goldberg at MikeGold60137@yahoo.com, at least five (5) days prior to the program, so that reasonable accommodation can be made for them.

**CONFIRMED Meeting dates for 2005 at Glenside Public Library:
May 28, June 18 CAEUG Picnic**

****NEW**** CD OF THE MONTH FORMAT: Is now available in **two (2)** flavors. The **Basic CD** will be packed with the standard items, while the **CD of the Month** will have NEW and updated items. Both are available at the meeting.

Presenter to be announced

Hope to see you there.

CAEUG website has a new home.

Remember to change your bookmark to the new address.

<http://www.caeug.net>